Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE GENERALIZED LAGRANGE INDETERMINATE CONGRUENCE FOR A COMPOSITE IDEAL MODULUS.

By H. S. Vandiver.

The present paper is devoted to certain generalizations of the relation

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1}-1 \pmod{p}, \tag{1}$$

p being a rational prime, and x an indeterminate quantity. In this connection Bauer* gave a formula involving a modulus which was a power of a rational prime. Proceeding along this line, but by a different method, we obtain extensions to cover residues with respect to any composite ideal modulus.

1. It is known† that if $\mathfrak{m}$ is an ideal in an algebraic field Ω, then the incongruent residues, modulo $\mathfrak{m}$, which are prime to $\mathfrak{m}$ (called a complete system of unit residues and denoted by C.S.U.R.) are given by

$$T_1\rho_1 + T_2\rho_2 + \cdots + T_k\rho_k, \tag{3}$$

where T_s ranges over a C.S.U.R. modulo $\mathfrak{p}_s^{a_s}$, $\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}$, $\rho_s \equiv 0 \pmod{\mathfrak{m}/\mathfrak{p}_s^{a_s}}$, $s = 1, 2, \cdots, k$, and $\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_k^{a_k}$, the $\mathfrak{p}$'s being distinct prime ideals in Ω.

Let x be an indeterminate and consider the product $\Pi(x-U)$, where U ranges over the set (3). Now the form of (3) shows that

$$\Pi(x-U) \equiv \Pi(x-T_s)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s^{a_s})} \pmod{\mathfrak{p}_s^{a_s}}. \tag{4}$$

To reduce the right-hand member we observe that a C.S.U.R. of $\mathfrak{p}_s^{a_s}$ (which for the present will be written $\mathfrak{p}^a$) is given by‡

$$R_1 + \theta R_2 + \theta^2 R_3 + \cdots + \theta^{a-1}R_a, \tag{5}$$

where θ is an algebraic integer in Ω divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$, and is furthermore prime to $\mathfrak{m}/\mathfrak{p}^a$, R_1 ranges over a C.S.U.R. modulo $\mathfrak{p}$, and each of the other R's runs through a complete system of residues, modulo $\mathfrak{p}$.

Reduce the right-hand member of (4) modulo $\mathfrak{p}$. By (5) it becomes

$$\Pi(x-R_1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p})},$$

modulo $\mathfrak{p}$. But we have§

---

* Nouvelles Annales de Mathematiques, series 4, vol. 2. See relation (10) of the present paper.

† Dirichlet-Dedekind, Zahlentheorie, 4th edition, pp. 568–9.

‡ Hilbert, Die Theorie der Algebraischen Zahlkörpers, p. 193.

§ Dirichlet-Dedekind, l. c., p. 570.

$$(6) \qquad \Pi(x - R_1) \equiv x^{\phi(\mathfrak{p})} - 1 \pmod{\mathfrak{p}}.$$

Modulo $\mathfrak{p}^2$, (4) reduces to

$$\Pi(x - S)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}^2)},$$

where S ranges over a C.S.U.R., modulo $\mathfrak{p}^2$. Write

$$\Pi(x - R_1) = \psi(x, \mathfrak{p}),$$

then

$$\Pi(x - (R_1 + R_2\theta)) \equiv \prod_t \psi(x - t\theta, \mathfrak{p}) \pmod{\mathfrak{p}^2},$$

where t ranges over a complete system of residues modulo $\mathfrak{p}$. We denote by $\mathfrak{p}f(x)$ a function of x in Ω, each of whose coefficients is divisible by the ideal $\mathfrak{p}$. We can then write

$$\psi(x, \mathfrak{p}) = x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p}f(x).$$

We have by Taylor's theorem

$$\psi(x - t\theta) \equiv \psi(x) - t\theta\frac{d\psi}{dx} \pmod{\mathfrak{p}^2},$$

and therefore

$$\psi(x - t\theta, \mathfrak{p}) \equiv x^{\phi(\mathfrak{p})} - \varphi(\mathfrak{p})x^{\phi(\mathfrak{p})-1}t\theta - 1 + \mathfrak{p}f(x) \pmod{\mathfrak{p}^2},$$

$$\prod_t [\psi(x - t\theta, \mathfrak{p})] \equiv (x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p}f(x))^{N(\mathfrak{p})} - (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})-1}\theta\varphi(\mathfrak{p})x^{\phi(\mathfrak{p})-1}\Sigma t \pmod{\mathfrak{p}^2},$$

where $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$.

In the relation (6) develop the left-hand member and equate coefficients of each side. We get $\Sigma t \equiv 0 \pmod{\mathfrak{p}}$, provided $N(\mathfrak{p}) \neq 2$. With this restriction on $\mathfrak{p}$ we have after further reduction

$$\prod_t [\psi(x - t\theta, \mathfrak{p})] \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2}.$$

If $\mathfrak{m}$ is divisible by $\mathfrak{p}^n$, (4) becomes, modulo $\mathfrak{p}^n$,

$$\Pi(x - T)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}^n)},$$

where T ranges over a C.S.U.R. modulo $\mathfrak{p}^n$. Assume that for a particular n

$$\Pi(x - T) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} \pmod{\mathfrak{p}^n}.$$

We shall then show that it necessarily follows from this assumption that

$$\Pi(x - T_1) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^n)} \pmod{\mathfrak{p}^{n+1}},$$

where T_1 ranges over a C.S.U.R. modulo $\mathfrak{p}^{n+1}$, and since the assumption holds for $n = 1$ and 2, it follows by induction that it is true for any positive integer n. If

$$\Pi(x - T) = \psi(x),$$

then

$$\Pi(x - T_1) = \prod_t \psi(x - t\theta^n),$$

where t ranges over a complete set of incongruent residues modulo $\mathfrak{p}$.

Let

$$\psi(x) = (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x),$$

where $\mathfrak{p}^n f(x)$ denotes a function of x in Ω, each of whose coefficients are divisible by $\mathfrak{p}^n$. Then for a fixed t

$$\begin{aligned}\psi(x - t\theta^n) &= [(x - t\theta^n)^{\phi(\mathfrak{p})} - 1]^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x - t\theta^n)\\ &\equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{n-1})} + \mathfrak{p}^n f(x) \pmod{\mathfrak{p}^{n+1}},\end{aligned}$$

and

$$\prod_t \psi(x - t\theta^n) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^n)} \pmod{\mathfrak{p}^{n+1}},$$

the desired result.

Using (4) we then have

$$\begin{aligned}\Pi(x - U) &\equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p}^{a-1}) \times \phi(\mathfrak{m})/\phi(\mathfrak{p}^a)} \pmod{\mathfrak{p}^a}\\ &\equiv (x^{\phi(\mathfrak{p})} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p})} \pmod{\mathfrak{p}^a}.\end{aligned}$$

We may then write

$$\Pi(x - U) \equiv \sum_{s=1}^{k} \rho_s (x^{\phi(\mathfrak{p}_s)} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s)} \pmod{\mathfrak{m}}, \tag{8}$$

where

$$\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}, \qquad \rho_s \equiv 0 \pmod{\mathfrak{m}/\mathfrak{p}_s^{a_s}}.$$

2. Now consider the case where $N(\mathfrak{p}) = 2$, which was excluded from the previous discussion. Suppose 2 is divisible by the prime ideal $\mathfrak{p}$, but not by $\mathfrak{p}^2$. Then we may take $2 = \theta$. Write

$$\Pi(x - T) = \psi(x, \mathfrak{p}^n),$$

where T ranges over a C.S.U.R. modulo $\mathfrak{p}^n$. Then

$$\begin{aligned}\psi(x, \mathfrak{p}^2) &\equiv (x - 1)(x - (1 + 2)) \pmod{4}\\ &\equiv (x^2 - 1) \pmod{4},\\ \psi(x, \mathfrak{p}^3) &\equiv \psi(x, \mathfrak{p}^2)\psi(x - 4, \mathfrak{p}^2) \pmod{8}\\ &\equiv (x^2 - 1)^2 \pmod{8},\end{aligned}$$

and in general

$$\psi(x, \mathfrak{p}^n) \equiv (x^2 - 1)^{\phi(\mathfrak{p}^n)/2} \pmod{\mathfrak{p}^n}, \tag{9}$$

where $n > 1$.

Suppose that 2 is divisible by $\mathfrak{p}^2$. Then proceeding as above, we find, if θ is an algebraic integer in Ω divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$,

$$\psi(x, \mathfrak{p}^2) = (x - 1)^2 - \theta(x - 1) + \mathfrak{p}^2 f(x),$$

and using

$$\psi(x, \mathfrak{p}^3) \equiv \psi(x, \mathfrak{p}^2)\psi(x - \theta^2, \mathfrak{p}^2) \pmod{\mathfrak{p}^3},$$

we get

$$\psi(x, \mathfrak{p}^3) \equiv [(x - 1)^2 - \theta(x - 1)]^2 \pmod{\mathfrak{p}^3}.$$

Similarly,

$$\psi(x, \mathfrak{p}^4) \equiv (x^2 - 1)^4 \pmod{\mathfrak{p}^4},$$

and in general we get (9) for $n > 3$.

3. By using methods similar to those employed above we can show that

$$\Pi(x - U') \equiv \sum_{s=1}^{k} \rho_s (x^{N(\mathfrak{p}_s)} - x)^{N(\mathfrak{m})/N(\mathfrak{p}_s)} \pmod{\mathfrak{m}}, \tag{8'}$$

where U' ranges over all the incongruent residues modulo $\mathfrak{m}$, and $N(\mathfrak{p}_s) \neq 2$.

Let

$$\omega(x, \mathfrak{p}^n) = \Pi(x - T'),$$

where T' ranges over all the incongruent residues modulo $\mathfrak{p}^n$, when $N(\mathfrak{p}) = 2$.

We have, if 2 is divisible by $\mathfrak{p}$, but not by $\mathfrak{p}^2$,

$$\begin{aligned} \omega(x, \mathfrak{p}^2) &\equiv x(x-1)(x-2)(x-(1+2)) \pmod{\mathfrak{p}^2} \\ &\equiv (x^2-1)(x^2-2x) \pmod{\mathfrak{p}^2}, \\ \omega(x, \mathfrak{p}^3) &\equiv \omega(x, \mathfrak{p}^2)\omega(x-4, \mathfrak{p}^2) \pmod{\mathfrak{p}^3} \\ &\equiv (x^2-1)^2(x^2-2x)^2 \pmod{\mathfrak{p}^3}, \end{aligned}$$

and in general

$$\omega(x, \mathfrak{p}^n) \equiv [(x^2-1)(x^2-2x)]^{\frac{N(\mathfrak{p}^n)}{4}} \pmod{\mathfrak{p}^n}, \tag{9'}$$

where $n > 1$. Similarly, if 2 is divisible by $\mathfrak{p}^2$, we obtain (9′) for $n > 3$.

By means of (8), (8′), (9), (9′) we can express in a simplified form any elementary symmetric function formed by all the incongruent unit residues modulo $\mathfrak{m}$, or any function of the same type formed by all the incongruent residues modulo $\mathfrak{m}$, where $\mathfrak{m}$ is *any* ideal in Ω. In particular, putting $x = 0$ in (8) we have

Theorem I. *The product formed by the set of all incongruent unit residues modulo* $\mathfrak{m}$, *an ideal in an algebraic field* Ω, *prime to* 2, *is congruent to minus unity or unity modulo* $\mathfrak{m}$, *according as* $\mathfrak{m}$ *possesses one or more than one distinct ideal prime factor.*

This is evidently a generalization of Wilson's theorem. The results of (8) and (8′) may be expressed by

Theorem II. *If* $\mathfrak{m}$ *is an ideal in an algebraic field* Ω, *and*

$$\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_k^{a_k} \qquad (N(\mathfrak{p}_s) \neq 2),$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$ *are distinct prime ideals in* Ω, *then*

$$\Pi(x - U) \equiv \sum_{s=1}^{k} \rho_s (x^{\phi(\mathfrak{p}_s)} - 1)^{\phi(\mathfrak{m})/\phi(\mathfrak{p}_s)} \pmod{\mathfrak{m}},$$

where U *ranges over all incongruent unit residues modulo* $\mathfrak{m}$, *and*

$$\Pi(x - U') \equiv \sum_{s=1}^{k} \rho_s (x^{N(\mathfrak{p}_s)} - x)^{N(\mathfrak{m})/N(\mathfrak{p}_s)} \pmod{\mathfrak{m}},$$

where U' ranges over all the incongruent residues modulo $\mathfrak{m}$. The ρ's are defined by

$$\rho_s \equiv 1 \pmod{\mathfrak{p}_s^{a_s}}, \qquad \rho_s \equiv 0 \quad \left(\mathrm{mod}\, \frac{\mathfrak{m}}{\mathfrak{p}_s^{a_s}}\right),$$

$s = 1, 2, \cdots, k$. *Further, x is an indeterminate, $\varphi(k)$ is the indicator of k, and $N(k)$ denotes the norm.*

If we suppose that Ω is the field of rational numbers, then the relations (8) and (8′) may be written (if the modulus $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where the p's are prime)

$$\Pi(x - U) \equiv \sum_{s=1}^{k} (m/p_s^{a_s})^{\phi(p_s^{a_s})} (x^{\phi(p_s)} - 1)^{\phi(m)/\phi(p_s)} \pmod{m}, \tag{10}$$

$$\Pi(x - U') \equiv \sum_{s=1}^{k} (m/p_s^{a_s})^{\phi(p_s^{a_s})} (x^{p_s} - x)^{m/p_s} \pmod{m}. \tag{11}$$

For the modulus $m = p^{a}$; the first relation was given by Bauer, as before noted.

4. Relations (8) and (8′) may be derived in a way a bit different from that previously used, by extending a method employed by Bauer in the article cited. Retaining the former notation, consider

$$\prod_{R_2}(x - (r + R_2\theta)) \pmod{\mathfrak{p}^2},$$

where r is fixed. This reduces to

$$(x - r)^{N(\mathfrak{p})} - (x - r)^{N(\mathfrak{p})-1} \Sigma R_2 \theta \pmod{\mathfrak{p}^2},$$

and (6) gives $\Sigma R_2 \equiv 0 \pmod{\mathfrak{p}}$, unless $\phi(\mathfrak{p}) = 1$, or $N(\mathfrak{p}) = 2$. With this exception the above expression becomes

$$(x - r)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2},$$

and by (6)

$$\prod_{r} (x - r)^{N(\mathfrak{p})} = (x^{\phi(\mathfrak{p})} - 1 + \mathfrak{p} f(x))^{N(\mathfrak{p})},$$

or

$$\Pi\,(x - (R_1 + R_2\theta)) \equiv (x^{\phi(\mathfrak{p})} - 1)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2}.$$

Using a method similar to the above we derive (8) by induction after employing (4). The relation (8′) follows in like manner.